UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

UNITED STATES OF AMERICA,	)	DOCKET NO. 3:13cr333-RJC
	)	
v.	)	SUPERSEDING BILL OF INDICTMENT
	)	
	)	
	)	18 U.S.C. § 1349
(1) VINICIO JOSEPH GONZALEZ,	)	18 U.S.C. § 2320(a)
a/k/a "Vinnie Gonzalez,"	)	
(2) HUGO REBAZA, JR., and	)	
(3) NASHANCY JOHNNY COLBERT,	)	
	)	
Defendants.	)	
	)	
_____	)	

THE GRAND JURY CHARGES:

At all times relevant to this Superseding Indictment:

INTRODUCTION

1. From at least in or around 2012, through in or about 2013, in Mecklenburg County, in the Western District of North Carolina, and elsewhere, Defendant VINICIO JOSEPH GONZALEZ, a/k/a "Vinnie Gonzalez", Defendant HUGO REBAZA, JR., Defendant NASHANCY JOHNNY COLBERT, Sean Roberson and other persons known and unknown to the Grand Jury, conspired to, and did, engage in a scheme and artifice to defraud and to obtain money and property from merchants, financial institutions and other financial service companies by manufacturing, distributing, receiving and using counterfeit credit cards and counterfeit debit cards ("counterfeit payment cards") bearing one or more registered trademarks for use with stolen credit card account numbers and stolen debit card account numbers ("stolen payment card account numbers") encoded onto the magnetic stripes of the counterfeit payment cards, thereby causing losses exceeding $30 million.

2. Sean Roberson ("Roberson"), an unindicted co-conspirator herein, was a resident of Palm Bay, Florida. Roberson was the owner and operator of a membership-only, e-commerce business and website, known as fakeplastic.net (the "Fakeplastic Website"), that sold counterfeit payment cards to its members-only customers, as well as holographic overlays used to make fake identification cards.

3. Defendant VINICIO JOSEPH GONZALEZ, a/k/a "Vinnie Gonzalez" ("GONZALEZ") was a resident of Palm Bay, Florida. Defendant GONZALEZ was an employee of the Fakeplastic Website who was primarily responsible for manufacturing counterfeit payment cards, packaging counterfeit payment cards and holographic overlays for mailing, and placing U.S. Express Mail envelopes in the United States mail for delivery to the members-only customers of the Fakeplastic Website.

4. Defendant HUGO REBAZA, JR. ("REBAZA") was a resident of Palm Bay, Florida. Defendant REBAZA was a part-time employee of the Fakeplastic Website who primarily picked up packages containing proceeds and supplies from a "mail drop" for the Fakeplastic website.

5. Defendant NASHANCY JOHNNY COLBERT ("COLBERT") was a resident of Charlotte, North Carolina. COLBERT was a members-only customer of the Fakeplastic Website who placed and received orders of counterfeit payment cards and counterfeit holograms delivered to COLBERT through the United States mail.

DEFINITIONS

6. As used in this Superseding Indictment, the following terms are defined as:

a. "Merchants" refers to retail establishments and businesses that sell consumer goods, wares, merchandise, prepaid payment cards and services to consumers at physical locations, referred to in the trade as bricks-n-mortar retail establishments. More than three million merchants in the United States accept electronic payments utilizing one or more electronic payment networks.

b. "Point of Sale Terminal" ("POS") means a Point-Of-Sale electronic device located within bricks-n-mortar retail establishments for acceptance of card-based electronic payments in exchange for consumer goods, wares, merchandise, prepaid payment cards, services and, in some cases, for the disbursement of cash to customers of merchants. Today, the vast majority of POS terminals in the United States read electronic payment data only from magnetic-stripe payment cards.

c. "Electronic Funds Transfer" ("EFT") is a payment systems industry term used to describe a broad range of technologies involving the electronic transfer of funds among financial institutions, typically using computers and telecommunications.

d. "EFT-POS payment systems" means Electronic Funds Transfer Payment Systems that use Point-of-Sale terminals to transmit and cause to be transmitted by wire communications in interstate commerce writings, signs, signals and sounds in connection with payment card transactions, including payment card account information and payment authorization information or payment declination information from card payment networks , including Visa, MasterCard, American Express and Discover, and from payment card issuers, typically financial institutions or financial services company.

e. "Credit Card" is an “access device” as defined in Title 18, United States Code, §1029(e)(1), that usually is a magnetic-stripe plastic card enabling the cardholder to (i) effect transactions on credit for consumer goods, wares, merchandise, prepaid payment cards, and services which are paid on behalf of the card holder by the issuer of such device or (ii) obtain cash with credit extended by the issuer. Visa, MasterCard and Discover are examples of branded Credit Cards.

f. "Charge Card" or "Travel and Entertainment Card" or "T&E Card" is an access device as defined in Title 18, United States Code, §1029(e)(1), that usually is a magnetic-stripe plastic card, enabling the cardholder to purchase on credit consumer goods, wares, merchandise, prepaid payment cards, and services to be paid on behalf of the cardholder by the issuer of such device. Typically, the contractual terms of such cards require that payment from the cardholder to the issuer be made in full each month, for all payments made on behalf of the cardholder by the issuer during the preceding month. The issuer does not extend credit to the holder beyond the date of the monthly statement, nor does it impose interest charges on the balance due except as a penalty for late payment. American Express is an example of a branded Charge Card.

g. "Debit Card" is an access device as defined in Title 18, United States Code, §1029(e)(1), that usually is a magnetic-stripe plastic card, enabling the cardholder, among other things, to make a purchase at a Point-Of-Sale Terminal which is debited against one or more of the cardholder's bank accounts, and to effect a cash withdrawal from the cardholder's bank account at a Point-Of-Sale Terminal in connection with a purchase from a merchant or at ATM (Automated Teller Machine) Terminal.

h. "POS Debit Card" is a debit card used at merchant Point-Of-Sale Terminals to purchase consumer goods, wares, merchandise, prepaid payment cards, and services, and to effect a cash withdrawal at a Point-Of-Sale Terminal in connection with a purchase from a merchant. A bank or other financial institution may issue a single magnetic-stripe plastic card which will function as both a POS debit card and an ATM card. VISA and MasterCard payment networks offer consumers POS Debit Cards.

i. “Payment Card” means a Credit Card, Charge Card, Debit Card and POS Debit Card.

j. "Magnetic-Stripe Plastic Card" means an access device containing a magnetic stripe which enables the cardholder to perform the functions or obtain the access provided by one or more of the Payment Cards defined above.

k. "Registered Trademark" means a mark (known in the trade as a “brand)) that is used in connection with goods, including payment cards, and services, including Electronic Fund Transfer payment system services, and registered on the principal register in the United States Patent and Trademark Office (“USPTO”).

l. "Card-Present POS Payment Card Authorization" means a payment card transaction authorization process in which the payment card issuer that issued the cardholder's payment card verifies that there are sufficient funds available in the cardholder's credit account or debit account to pay the amount of the retail purchase and electronically "puts a hold" on those funds in during the retail transaction payment process. The payment card authorization process also includes a software-based fraud risk analysis that provides a fraud risk score whether the payment transaction involves the genuine cardholder or an imposter. The payment card authorization process typically is performed in ten (10) seconds or less.

m. "Card-Present POS Payment Card Declination" means a payment card transaction authorization process in which the payment card issuer that issued the cardholder's payment card has verified that there are insufficient funds available in the cardholder's credit account or debit account to pay the amount of the retail purchase and electronically, that there is high fraud risk score indicating a high probability that an imposter is posing as the genuine cardholder, or that the genuine cardholder has notified the cards issuer that the payment card account information has been stolen or otherwise compromised. Typically, merchants are not advised in the electronic payment process regarding the reason for a declined electronic payment.

n. "Card Issuing Institution" means a bank, other financial institution, or other financial services company that uses the Visa, MasterCard, American Express or Discover Electronic Funds Transfer payment systems and networks and that issues Visa, MasterCard, American Express or Discover branded magnetic-stripe plastic payment cards to consumers for their use in electronic payment systems.

o. “Acquiring Institution" or "Merchant Institution" means a bank, other financial institution, or other financial services company that establishes agreements with Merchants whereby Merchants agree to accept Visa, MasterCard, American Express or Discover branded magnetic-stripe plastic payment cards as payment for the credit consumer goods, wares, merchandise, prepaid payment cards, and services that they sell to consumers.

p. “Track data” refers to data that is encoded on the magnetic stripe on the back of a payment card. Track data contains certain information relating to a particular credit or debit account, including the credit or debit account number and the name on the account. Criminals often refer to stolen track data as “dumps.”

q. “Embossing” is the act of printing certain information on payment cards. Embossed print is the raised print typically appearing on the face of legitimate payment cards that displays information associated with a particular card, such as the name of the accountholder, the account number for the account, and expiration date for the card.

r. "Authentication features" refer to any hologram, watermark, certification, symbol, code, image, sequence of numbers or letters, or other feature that either individually or in combination with another feature is used by the issuing authority on an identification document, document-making implement, or means of identification to determine if the document is counterfeit, altered, or otherwise falsified.

s. "Liberty Reserve" is an online currency, which, until in or around May 2013, could be used to pay for goods or services over the Internet, and could be exchanged into United States currency.

t. "Bitcoin" is a cryptographic-based digital currency, which can be used to pay for goods or services over the Internet, and can be exchanged into United States currency through the use of Bitcoin exchangers.

u. "Skimming operations" refer to schemes involving the installation of specialized equipment at either ATM locations or Point-Of-sale Terminals designed to steal payment card information at the time it is used by a genuine payment card holder at ATMs and POS terminals.

v. "Hacking" refers to the software intrusion or data breach of a computer system to steal sensitive information, including payment card account information of consumers.

CARD-BASED EFT PAYMENT NETWORKS

7. Most consumers in the United States used magnetic-stripe payment cards to pay for consumer goods, wares, merchandise, prepaid payment cards and services purchased from merchants, and in connection with some purchase transactions, for receipt of cash back from merchants.

8. Magnetic-stripe payment cards were plastic cards that contained visible payment card account information on the front of the payment card and electronic payment card account information encoded onto a magnetic stripe on the back of the payment card. Magnetic-stripe plastic payment cards typically contained graphic designs featuring one or more registered trademarks of at least one card payment network, including Visa, MasterCard, American Express and Discover.

9. Visa, Inc. ("Visa"), MasterCard Incorporated ("MasterCard"), American Express Company ("American Express") and Discover Financial Services ("Discover") were financial service companies that operated their own independent EFT payment card networks.

10. VISA, MasterCard, American Express and Discover owned and had licensing rights to one or more trademarks registered in the principal registry in the United States Patent and Trademark Office, including respectively, but not limited to, the Registered Trademarks:

a. "VISA"
b. "MasterCard"
c. "American Express" and
d. "Discover"

SCHEME AND ARTIFICE

11. Sean Roberson created, designed and operated the Fakeplastic Website as a members-only, e-commerce website to enable criminals to browse, order and purchase from an extensive inventory of genuine-looking, but counterfeit, magnetic-stripe plastic payment cards ("counterfeit payment cards") ready to be encoded with stolen payment card data onto the magnetic stripes of the counterfeit payment cards. Stolen payment card data is known in the illegal underground of various carding forums as track data or card "dumps."

12. The Fakeplastic Website required that its customers become members of the Fakeplastic Website through sponsorship by criminals who sold stolen payment card account information in numerous illegal online carding forums or by existing Fakeplastic Website members.

13. Once accepted as a members-only customer of the Fakeplastic Website (hereinafter "Fakeplastic customers"), Fakeplastic customers could and did enter unique username IDs and associated passwords on the homepage of the Fakeplastic Website, and thereafter could and did access the Fakeplastic Website's online display of an extensive inventory of counterfeit payment cards and counterfeit holographic overlays.

14. Fakeplastic customers could and did select the type and quantity of counterfeit payment cards and counterfeit holographic overlays they wished to purchase. For an additional fee, Fakeplastic customers could and did order custom embossing on the face of the counterfeit payment cards to include information typically associated with genuine payment cards, including cardholder names, payment card account numbers, and payment card expiration dates.

15. Fakeplastic customers typically paid for their orders of counterfeit payment cards and counterfeit holographic overlays using Liberty Reserve, Bitcoin and, in some cases, cash.

16. On a daily basis, Sean Roberson downloaded the orders of Fakeplastic customers and delivered the orders to defendant GONZALEZ.

17. On a daily basis, defendant GONZALEZ processed the Fakeplastic customer orders.

18. Defendant GONZALEZ processed orders of unembossed counterfeit payment cards by matching customer orders with the digital inventory of Fakeplastic's counterfeit payment cards, and using a specialized printer to print the counterfeit payment cards onto plain-white magnetic-stripe cards.

19. Defendant GONZALEZ processed orders of embossed counterfeit payment cards by matching customer orders with the digital inventory of Fakeplastic's counterfeit payment cards, using a specialized printer to print the counterfeit payment cards onto plain-white magnetic stripe cards, and using a computerized embossing device to custom emboss the counterfeit payment cards ordered by Fakeplastic customers.

20. Defendant GONZALEZ further processed orders of unembossed and embossed counterfeit payment cards, and counterfeit holograms, by packaging the customized orders of counterfeit payment cards and counterfeit holograms into U.S. Express Mail envelopes.

21. Defendant GONZALEZ placed into the U.S. mail hundreds of U.S. Express Mail envelopes containing tens-of-thousands of counterfeit payment cards and thousands of counterfeit holograms for delivery to Fakeplastic customers.

22. The Fakeplastic Website utilized the tracking features of U.S. Express Mail to enable Fakeplastic customers to track the status of the transportation and delivery of the U.S. Express Mail envelopes containing the counterfeit payment card orders of Fakeplastic customers.

23. Upon receipt of the Fakeplastic Website's unembossed counterfeit payment cards, Fakeplastic customers would and did emboss the front face of the counterfeit payment cards to include information typically associated with genuine payment cards, including cardholder names, payment card account numbers, and payment card expiration dates. The Fakeplastic customers who purchased unembossed counterfeit payment cards also would and did encode stolen payment cards data onto the magnetic stripes of the counterfeit payment cards.

24. Upon receipt of the Fakeplastic Website's embossed counterfeit payment cards, Fakeplastic customers would and did encode stolen payment cards data onto the magnetic stripes of the counterfeit payment cards.

25. Fakeplastic customers and other conspirators to whom Fakeplastic customers transferred or sold counterfeit payment cards containing stolen payment card information would and did use the counterfeit payment cards at merchant locations to purchase consumer goods, wares, merchandise, prepaid payment cards, services and, in some cases, to obtain cash from merchants.

26. The Fakeplastic Website's counterfeit payment cards typically bore at least one of the Registered Trademarks of Visa, MasterCard, American Express or Discover.

27. The Fakeplastic Website's counterfeit payment cards were high quality counterfeit payment cards that were substantially indistinguishable from genuine payment cards issued by the EFT card payment networks.

28. The Fakeplastic Website's counterfeit payment cards containing stolen payment card account information encoded onto the magnetic stripe of the counterfeit payment cards would and did deceive employees of merchants in electronic payment transactions at POS terminals.

29. The stolen payment card account information encoded on the magnetic stripe of the counterfeit payment cards was used on Point-of-Sale Terminals and processed by the EFT-POS payment system, including by Acquiring or Merchant Institutions, Card Issuing Institutions and Card Payment networks, to complete card-present purchase transactions at merchant locations.

30. Electronic payment transactions executed at Merchant POS Terminals with the Fakeplastic Website's counterfeit payment cards encoded with stolen payment card account information typically were authorized where sufficient credit lines or funds were available in associated card accounts to cover the electronic payment transactions, and where card payment networks failed to compute a high fraud risk score or the genuine cardholder had not notified the Card Issuing Institution of any prior unauthorized fraudulent charges.

COUNT ONE
(Conspiracy to Traffic in Counterfeit Goods – 18 U.S.C. §2320(a))

31. Paragraphs 1 through 30 of this Superseding Indictment are re-alleged and incorporated herein by reference as though fully set forth herein.

32. From at least as early as in or about 2012 through in or about 2013, in the Western District of North Carolina, and elsewhere, defendants

VINICIO JOSEPH GONZALEZ,
a/k/a "Vinnie Gonzalez," and
HUGO REBAZA, JR.,

knowingly and intentionally conspired and agreed with each other and with Sean Roberson and with others known and unknown to the Grand Jury to traffic and attempt to traffic in goods and services and knowingly used counterfeit marks on and in connection with such goods and services, and intentionally trafficked and attempted to traffic in labels, patches, stickers, wrappers, badges, emblems, medallions, charms, boxes, containers, cans, cases, hangtags, documentation, and packaging of any type and nature, knowing that counterfeit marks had been applied thereto, the use of which was likely to cause confusion, to cause mistake, and to deceive.

Object of the Conspiracy

33. It was an object of the conspiracy for the defendant, **VINICIO JOSEPH GONZALEZ, a/k/a "Vinnie Gonzalez,"** Defendant **HUGO REBAZA**, JR., Sean Roberson and others known and unknown to the Grand Jury to unlawfully enrich themselves by trafficking and attempting to traffic in counterfeit payment cards that bore one or more Registered Trademarks owned by VISA, MasterCard, American Express and Discover without the authorization of the card payment networks, a violation of Title 18, United States Code, Section 2320(a).

Manner and Means

34. The conspirators carried out the conspiracy in the manner and means described in paragraphs 1 through 30 of this Superseding Bill of Indictment, among others.

Overt Acts

35. In furtherance of the conspiracy and to effect the objects thereof, the following overt acts, among others, were committed in the Western District of North Carolina, and elsewhere:

a. Between on or about November 18, 2013, and on or about November 21, 2013, defendant **GONZALEZ** placed in the United States Mail a package containing counterfeit payment cards destined for and received in the Western District of North Carolina.

b. Between on or about November 21, 2013, and on or about November 25, 2013, defendant **GONZALEZ** placed in the United States Mail a package containing counterfeit payment cards destined for and received in the Western District of North Carolina.

c. On or about October 3, 2013, defendant **REBAZA** picked up a FedEx envelope from a Fakeplastic Website "mail drop" maintained at Atlantic Pack & Parcel in Indialantic, Florida.

All in violation of Title 18, United States Code, Section 2320(a).

COUNT TWO
(MAIL/WIRE/BANK FRAUD CONSPIRACY - 18 USC §1349)

36. Paragraphs 1 through 30 of this Superseding Indictment are re-alleged and incorporated herein by reference as though fully set forth herein.

37. From at least in or about 2012 through in or about 2013 , in Mecklenburg County, within the Western District of North Carolina, and elsewhere, the defendants,

VINICIO JOSEPH GONZALEZ,
a/k/a "Vinnie Gonzalez,"
HUGO REBAZA, JR., and
NASHANCY JOHNNY COLBERT,

did knowingly combine, conspire, confederate, and agree with each other and with other persons known and unknown to the Grand Jury, to commit one or more offenses against the United States, including violations of Title 18, United States Code, Section 1341 (mail fraud), Title 18, United States Code, Section 1343 (wire fraud) and Title 18, United States Code, Section 1344 (bank fraud).

Objects of the Conspiracy

38. ***Mail Fraud.*** It was a part and an object of the conspiracy that the defendants, and others known and unknown to the Grand Jury, having devised the above-described scheme and artifice to defraud and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did, in executing and attempting to execute said scheme, place in any post office or authorized depository for mail matter any matter or thing whatever to be sent or delivered by the Postal Service, or takes or receives therefrom any such matter or thing, or knowingly causes to be delivered by mail according to the direction thereon, or at the place at which it is directed to be delivered by the person to whom it is addressed, any such matter or thing, in violation of Title 18, United States Code, Section 1341.

39. ***Wire Fraud.*** It was a part and an object of the conspiracy that the defendants, and others known and unknown to the Grand Jury, having devised the above-described scheme and artifice to defraud and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did, in executing and attempting to execute said scheme, transmit and cause to be transmitted by means of wire communication in interstate commerce, writings, signs, signals, pictures, and sounds for the purposes of executing said scheme and artifice, in violation of Title 18, United States Code, Section 1343.

40. ***Bank Fraud.*** It was a part and an object of the conspiracy that the defendants, and others known and unknown to the Grand Jury, having devised the above-described scheme and artifice to defraud and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did execute and attempt to execute said scheme to defraud one or more financial institutions, and would and did execute and attempt to execute said scheme to obtain the moneys, funds, credits, and assets owned by and under the control of one or more financial institutions by means of false and fraudulent pretenses, representations or promises, in violation of Title 18, United States Code, Section 1344.

Manner and Means

41. The conspirators carried out the conspiracy in the manner and means described in paragraphs 1 through 30 of this Superseding Bill of Indictment, among others.

Overt Acts

42. In furtherance of the conspiracy and to effect the objects thereof, the following overt acts, among others, were committed in the Western District of North Carolina, and elsewhere:

a. Between on or about November 18, 2013, and on or about November 21, 2013, defendant **GONZALEZ** placed in the United States Mail a package containing counterfeit payment cards destined for and received in the Western District of North Carolina.

b. Between on or about November 21, 2013, and on or about November 25, 2013, defendant **GONZALEZ** placed in the United States Mail a package containing counterfeit payment cards destined for and received in the Western District of North Carolina.

c. On or about October 3, 2013, defendant **REBAZA** picked up a FedEx envelope from a Fakeplastic Website "mail drop" maintained at Atlantic Pack & Parcel in Indialantic, Florida.

d. On or about December 3, 2013, defendant **COLBERT** received a U.S. Express Mail envelope in Charlotte, North Carolina, from the Fakeplastic Website containing counterfeit payment cards.

e. On December 7, 2013, a conspirator used a Fakeplastic Website embossed counterfeit payment card encoded with stolen payment card account information on the magnetic stripe of the counterfeit payment card at a Charlotte-based merchant, resulting in a fraudulent electronic payment transaction.

All in violation of Title 18, United States Code, Section 1349.

NOTICE OF FORFEITURE AND FINDING OF PROBABLE CAUSE

Notice is hereby given of 18 U.S.C. §§ 981, 982, 1029, and 2323, 28 U.S.C. § 2461(c), and 21 U.S.C. § 853. Under Section 2461(c), criminal forfeiture is applicable to any offenses for which forfeiture is authorized by any other statute, including but not limited to 18 U.S.C. § 981 and all specified unlawful activities listed or referenced in 18 U.S.C. § 1956(c)(7), which are incorporated as to proceeds by Section 981(a)(1)(C). The following property is subject to forfeiture in accordance with Section 981, 982, 1029, 2323, 2461(c), and/or 853:

a. Any article, the making or trafficking of which is prohibited under Section 506 of Title 17, or Section 2318, 2319, 2319A, 2319B, 2320, or Chapter 90 of Title 18;

b. All property which constitutes or is derived from proceeds obtained directly or indirectly as a result of the violations set forth in this bill of indictment;

c. All property used, or intended to be used, in any manner or part to commit or facilitate the commission of the violations; and

d. If, as set forth in 21 U.S.C. § 853(p), any property described in (a), (b), or (c) cannot be located upon the exercise of due diligence, has been transferred or sold to, or deposited with, a third party, has been placed beyond the jurisdiction of the court, has been substantially diminished in value, or has been commingled with other property which cannot be divided without difficulty, all other property of the defendant/s to the extent of the value of the property described in (a), (b), and (c).

The Grand Jury finds probable cause to believe that the following property is subject to forfeiture on one or more of the grounds stated above:

a. Approximately $4800 seized on or about December 4, 2013 during execution of a search warrant at 1640 Los Palmos Drive, Palm Bay, Florida;

b. Approximately four Bitcoins held by or for the benefit of Vinicio Gonzalez;

c. The following electronic items seized during the investigation of this matter:

- One Samsung Notebook;
- One Apple Macbook;
- One Compaq Desktop, Model CQ5814;
- One Cannon Printer, Model MF4450;
- One Zebra Technologies Card Printer, Model P430i;
- One Fargo HDP 8500 Card Printer;
- Six Fargo HDP 5000 Card Printers;
- One DataCard Card Embosser, Model 1501;
- One Wonder Manual Embosser;
- One WTJ-90A Manual Tipper;

- One Manual Card Press; and

- Miscellaneous supplies used or intended to be used to facilitate the offenses set forth herein.

ANNE M. TOMPKINS
UNITED STATES ATTORNEY